Ricardo A. Vittoni - FSS

Nápoles 3139 - C1431DEA - Cdad. de Buenos Aires - Cel. (11) 15 4416-8977 - ravittoni@gmail.com

SISTEMAS DE SEGURIDAD PARA QUEMADORES (BMSIS)

SAFETY NOTE SN - 5031

EVALUACIÓN E IMPLEMENTACIÓN DEL NIVEL SIL NECESARIO PARA QUEMADORES

1. "Mitos" que siguen matando gente

Continuando con el análisis planteado en la Nota de Seguridad "SN-3121, Funciones Instrumentadas de Seguridad para Quemadores de Calderas y Hornos" (Dic. 2003), he visto la necesidad de analizar, en forma más precisa y objetiva, el Nivel de Riesgo al que están sometidas las personas que trabajan en la proximidad de Calderas y Hornos Industriales, habiendo observado que el análisis cualitativo, eminentemente subjetivo, utilizado por algunos responsables del diseño de Sistemas BMS (BMSIS), ha llevado a una subvaloración de este Nivel de Riesgo en muchas instalaciones, lo cual ha derivado en accidentes catastróficos, con muchas personas muertas, como el caso de Algeria (27 muertos y decenas de heridos graves), hace apenas un año, o el caso de Córdoba (4 muertos), acaecido hace sólo unos días en nuestro país.

Y esto se debe, fundamentalmente, a la existencia de "mitos" que hacen que los Responsables de Ingeniería y/o de Seguridad de algunas empresas procedan en forma equívoca causando, sin quererlo, mucho más daño del que creen estar evitando...

Entre los muchos de estos "mitos" que hemos encontrado en los últimos años, podemos mencionar los que se ven con mayor frecuencia (se subrayan los falsos conceptos que favorecen la divulgación del "mito"):

1) "No es necesario utilizar un PLC especial para el Sistema de Seguridad. Es suficiente con utilizar un PLC de marca reconocida"
   o... "Es suficiente con usar un controlador aprobado por NFPA"

2) "Las explosiones de calderas no son tan frecuentes, ¿por qué habría de pasarnos justo ahora a nosotros?"
3) "En nuestra planta no hay problema. En caso que se apague la llama siempre hay una persona que puede apretar el botón de emergencia"
4) "Un Sistema de seguridad como el que pretenden las Normas es demasiado caro"
5) "Por qué debiéramos poner ahora un Sistema diferente si hace años que usamos éste en todas nuestras calderas y nunca pasó nada?
6) "Por qué cambiar la forma en que siempre lo hicimos si nadie nos obliga?
7) "Nosotros confiamos en nuestros proveedores. Si ellos no nos han dicho nada hasta ahora es porque no es necesario cambiar nada"

No pretendo analizar en este momento cada uno de estos "mitos" pero sí quiero reafirmar que son solamente eso, mitos (según la Real Academia Española, "persona o cosa a las que se atribuyen cualidades o excelencias que no tienen, o bien una realidad de la que carecen").

Sí pretendo con este artículo, fundamentar objetivamente la solución correcta para proveer el Nivel de Reducción de Riesgo apropiado para este tipo de aplicaciones.

2. Diseño Conceptual de un Sistema de Seguridad para Quemadores (BMSIS)

Ha quedado demostrado ampliamente, que el mayor riesgo al que está sujeta una persona que desarrolla sus actividades en las proximidades de una Caldera (o de un Horno) Industrial, es la eventual explosión del hogar.

A tal punto, que el tiempo máximo, establecido como mandatorio y prescriptivo por la Norma FM 7605, para el cierre del paso de combustible en caso de detectarse la extinción de la llama del quemador, es de **tan sólo 4 segundos**.

Obviamente, para poder cumplir con esta prescripción, es absolutamente necesario detectar en forma inmediata la extinción de la llama, procesar en el menor tiempo posible esta señal y cortar en forma efectiva el paso del combustible, en **menos** de 4 segundos.

Nápoles 3139 - C1431DEA - Cdad. de Buenos Aires - Cel. (11) 15 4416-8977 - ravittoni@gmail.com

Una falla en cualquiera de estas acciones podrá producir una explosión del hogar de consecuencias muy graves o catastróficas, como las mencionadas anteriormente.
Es decir, el BMSIS tiene que operar con "**total certeza**" (en inglés "certainty"), a fin de garantizar su acción protectora en forma rápida, confiable y segura, es decir, con Seguridad Funcional ("Functional Safety").

El Nivel de Integridad Segura (SIL) requerido para esta Función de Seguridad (SIF), dependerá del nivel de riesgo tolerable establecido por el Usuario y del nivel de riesgo inherente al diseño de la Caldera (o del Horno).

Pero, ¿qué debe hacerse cuando el Usuario no tiene, no establece, o desconoce cuál es el valor de riesgo tolerable en su Planta, o cuando el valor que éste define es superior al nivel de riesgo aceptado por la legislación vigente?
Peor aún, ¿qué debe hacerse cuando no existe siquiera una definición de riesgo aceptable en esta última?

Existen a estas preguntas tres respuestas posibles:

a) La caldera (o el horno) no podrá ponerse en servicio (absurda).
b) Podrán emularse las medidas de seguridad utilizadas en otras calderas u hornos similares (con riesgo de subvalorar el verdadero Nivel de Riesgo, como ha sucedido en casos que derivan en accidentes graves como los mencionados en el punto 1).
c) Deberán realizarse los estudios adecuados para implementar la solución, **utilizando las herramientas y prácticas de ingeniería que hayan sido aceptadas internacionalmente sobre la base de la experiencia acumulada a lo largo de muchos años y de muchos accidentes**, es decir, seguir las Normas Internacionales de Prescripción y de Peformance.

Reiteramos entonces, que **la única forma de implementar un BMSIS que permita realmente prevenir la explosión de una Caldera** (o de un Horno), **es seguir "al pie de la letra" y simultáneamente, las Normas prescriptivas NFPA 85 (86), FM 7605 y FM 7610, así como la Norma IEC 61511, "Seguridad Funcional para Industrias de Proceso"**.

Lamentablemente, la aplicación de estas Normas no está explícitamente indicada por las Leyes de nuestro país, aunque uno de los principios básicos que establece la Ley 19587 de Higiene y Seguridad, es “la observancia de las recomendaciones internacionales en cuanto se adapten a las características propias del país y ratificación, en las condiciones previstas precedentemente, de los convenios internacionales en la materia".
Por este motivo, es muy probable que posteriores Resoluciones de la SRT o del MTESS incluyan la obligatoriedad de seguir dichas prescripciones y recomendaciones.

No obstante, considero muy importante que **asumamos su utilización HOY** aunque la Ley AÚN no nos "obligue" a usarlas.

Y es que tiene que ser **nuestro principal objetivo**, en el ambiente industrial donde se instalen y funcionen calderas y hornos, **salvaguardar la vida humana** (evaluando los Niveles de Riesgo e implementando los medios técnicos necesarios para reducirlos en forma efectiva), **a lo largo de todo el Ciclo de Vida de las instalaciones**.

3. Evaluación del Nivel de Riesgo utilizando el Gráfico de Riesgo Calibrado

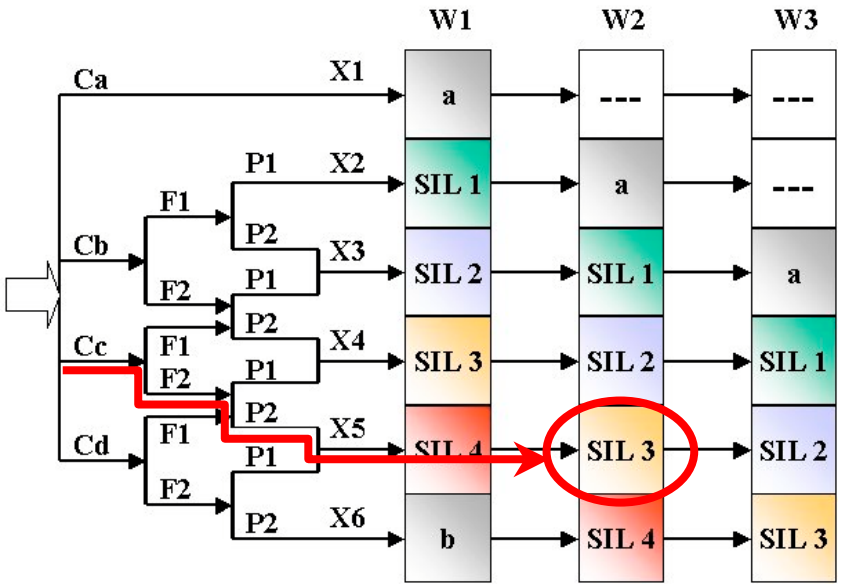
La Norma IEC 61511 establece que, cuando no sea posible calcular en forma precisa el Nivel de Riesgo, deberán utilizarse métodos que permitan aproximarse a este valor lo más posible y "redondear hacia arriba", es decir, que ante la menor duda entre tomar un Nivel de Riesgo menor y otro mayor, **se deberá tomar siempre el Nivel de Riesgo mayor**.

Volviendo a nuestra propuesta del principio (es decir, la de encontrar la forma de aproximar cuantitativamente nuestro análisis a fin de evitar catastróficas "evaluaciones cualitativas" o "presunciones"), hemos elegido utilizar el método conocido como "Calibrated Risk Graph" (Gráfico de Riesgo Calibrado), propuesto originalmente por la Norma IEC 61508 y recomendado por la Norma IEC 61511-3, "Guía para la Determinación de los Requeridos Niveles de Integridad de la Seguridad".

El esquema de la página siguiente muestra el Gráfico de Riesgo utilizado para calcular el Nivel de Riesgo del Operador de una Caldera Industrial y, consecuentemente, el Nivel SIL de la "SIF de shut-off de quemadores por apagado de llama" correspondiente.

Al tratarse de un método semi-cualitativo (o semi-cuantitativo), los valores obtenidos deberán ser tomados como valores mínimos del Nivel SIL a implementar ("redondear hacia arriba"), a menos que estudios cuantitativos demuestren que este Nivel SIL pudiera ser inferior.

Se asumen los siguientes valores tomados de la referencia citada (IEC 61511-3), para los parámetros C (Consecuencia), F (Frecuencia), P (Probabilidad de Evitar el Daño) y W (Demanda):



Consecuencia = Cc

"Cc" significa que el **daño físico podrá resultar entre el 10% de incapacidad y la muerte** del Operador

Frecuencia = F2

"F2" significa que **el Operador permanece en el área de peligro durante al menos el 10% de su tiempo de permanencia en Planta** (considerando la probabilidad de una explosión, el área de

peligro será suficientemente grande como para alcanzar incluso a otras personas, pero se considera sólo el daño del Operador para simplificar el cálculo).

Probabilidad = P2

"P2" significa **probabilidad muy baja de evitar el daño al Operador** (entre el 10% de incapacidad y la muerte, según Cc), si el BMSIS fallara en su acción protectora (entre una de las cuatro condiciones que la IEC 61511 establece para determinar esta probailidad, se halla el tiempo que tendrá el Operador para ponerse a salvo, el cual deberá ser mayor que una hora para que esta probabilidad de evitar el daño pudiera considerarse como alta, es decir, P1).

Demanda = W2

"W2" es la frecuencia intermedia (ni muy alta ni muy baja) con que pudiera presentarse el peligro si no existiera el BMSIS, y que corresponde al rango comprendido **entre 1 demanda por año y 1 demanda cada 10 años** (se considera que este valor es adecuado para una Caldera o un Horno, siempre y cuando el Sistema de Control Regulatorio opere adecuadamente y su diseño sea tal que evite la introducción de condiciones de peligro adicionales, por ejemplo, durante el cambio de combustible en sistemas duales).

Como puede verse en el gráfico, el Nivel de Riesgo "X5" determinado por la combinación de los parámetros de riesgo Cc, F2 y P2 mencionados, para una frecuencia en la demanda de acción del sistema bastante conservadora, nos lleva a **tener que utilizar una SIF de Nivel SIL 3**.

Aún si nos hubiéramos equivocado en alguna de estas "aproximaciones", queda claramente visible en el gráfico que el Nivel SIL se halla entre los valores SIL 2 y SIL 4 (cuyo valor "promedio" también es SIL 3).
Es decir, si nos hubiéramos equivocado y el valor debiera ser SIL 4, no sólo estaríamos obligados a utilizar una SIF de Nivel SIL 3 sino que, además, deberíamos implementar otros medios de prevención independientes para poder cubrir este Nivel de Riesgo.
Si, por el contrario, nos hubieramos equivocado y el valor debiera ser SIL 2, el equipamiento requerido y su instalación serían prácticamente los mismos, como veremos a continuación.

4. Implementación de los Medios necesarios para reducir el Riesgo

A fin de preservar la Seguridad Funcional del "lazo de seguridad" (SIF), la IEC 61511 nos da una guía acerca de cuántos elementos de campo se requieren para cada Nivel SIL, sobre la base de su "fracción de falla segura", es decir, sobre qué porcentaje de las fallas de un equipo se puede considerar que éste no producirá en sí mismo una situación de riesgo.

Para comprender este concepto, tomemos por caso un Detector de Llama.
Como este detector está compuesto por circuitos electrónicos (incluso los más modernos utilizan microprocesadores), su funcionamiento está sujeto a fallas que podrán o no ser detectadas por el sistema de autodiagnóstico del detector.
Ante una duda de funcionamiento correcto, dicho sistema de autodiagnóstico enviará una señal al Logic Solver del BMSIS que hará disparar la SIF de protección.

Ahora bien:
¿Cuántas fallas, del total de fallas posibles de la electrónica del detector, es capaz de detectar su sistema de autodiagnóstico?
¿Cuántas de estas fallas, al no ser detectadas, podrán "engañar" al BMSIS haciéndole "creer" que está todo bien y producir una explosión?

La "fracción de falla segura" (SFF) de un equipo nos permite predecir este comportamiento, sobre la base del cual la IEC 61511 pone a nuestra disposición la siguiente tabla, que nos indica cuántos dispositivos (externos o internos) deberán utilizarse en el campo para garantizar una operación segura:

Para un Nivel SIL 2 → Tolerancia a Fallas 1
Para un Nivel SIL 3 → Tolerancia a Fallas 2

Lo cual significa que deberemos instalar, por ejemplo 2 ó 3 detectores de llama en votación, según el Nivel SIL.

Nápoles 3139 - C1431DEA - Cdad. de Buenos Aires - Cel. (11) 15 4416-8977 - ravittoni@gmail.com

La Norma también establece que si puede demostrarse que los dispositivos cumplen con requisitos de performance y seguridad funcional, se podrá mejorar (disminuir) la tolerancia a fallas requerida.

Dicho en otras palabras, para una SIF de Nivel SIL 3 deberán utilizarse 3 detectores de llama simples, o **dos detectores de llama de alta integridad compuestos, con "canales" independientes** (UV+IR), como ya analizáramos en la SN-3121.

Podemos hacernos entonces la pregunta "¿qué cambiaría realmente en el campo si tuviéramos que pasar una 'SIF de shutoff por falta de llama' de Nivel SIL 2 a Nivel SIL 3?", la respuesta es "prácticamente nada", es decir, utilizando elementos de la calidad adecuada, la solución **óptima para cualquiera de los dos Niveles SIL**, es utilizar **como mínimo**, 2 elementos de detección de llama, preferiblemente duales y 2 válvulas de shutoff o sistemas de válvula de "Triple Efecto".

¿Cambia entonces el Logic Solver que debemos utilizar? La respuesta es NO necesariamente.
Si se está utilizando un Logic Solver Failsafe que es solamente apto para SIL 2, su cambio por uno apto para SIL 3 implicará, en muchos casos, un gasto menor.

Pero si estamos en la etapa de diseño, **la selección de un Logic Solver FailSafe apto para SIL 3 no implicará un costo adicional** con respecto a uno que sea sólo apto para SIL 2.

La solución **óptima para cualquiera de los dos Niveles SIL**, es utilizar Logic Solvers con arquitectura dual 1oo2D (o Triple Redundantes 2oo3D, cuando el sistema requiera de muy alta disponibilidad), como también analizamos en la SN-3121.

5. Conclusiones

Asumamos, por todo lo expuesto, **que DEBEMOS prescribir, para toda Caldera u Horno Industrial, la utilización de un BMSIS con capacidad para ejecutar lazos de seguridad de Nivel SIL 3**, pues no existen razones técnicas ni de costo para no hacerlo.

Si así no lo hiciéramos, **correríamos el riesgo de ser nosotros mismos los culpables de un accidente que pudiera costar muchas vidas**.

Ricardo A. Vittoni - FSS
Functional Safety Specialist